1 (calcul général du groupe de Galois). Soit $p(t) = t^d + a_1 t^{d-1} + \cdots + a_d \in K[t]$ un polynôme (unitaire, de degré d) séparable à coefficients dans un corps K, et $\xi_1, \ldots, \xi_d$ (de sorte que $p(t) = \prod_{i=1}^d (t - \xi_i)$) ses racines dans son corps de décomposition qu'on notera L. On définit la *résolvante de Kronecker* de p comme

$$s(t) = \prod_{\sigma \in \mathfrak{S}_d} \Big(t - \sum_{i=1}^d u_i \xi_{\sigma(i)} \Big) \in L[u_1, \ldots, u_d, t]$$

(Imaginer que s est le polynôme en t dont les racines sont les combinaisons linéaires $\sum_i u_i \xi_{\sigma(i)}$ à coefficients des indéterminées u_i.) Montrer que s est, en fait, à coefficients dans K, et qu'il est invariant par $\mathfrak{S}_d$ (agissant par permutation sur les variables $u_1, \ldots, u_d$). Soit h un facteur irréductible[1] quelconque de s dans $K[u_1, \ldots, u_d, t]$ (on le prendra unitaire) : on considère le sous-groupe S_h de $\mathfrak{S}_d$ formé des permutations $\sigma \in \mathfrak{S}_d$ qui laissent h invariant. Montrer que S_h est conjugué, dans $\mathfrak{S}_d$, au groupe de Galois $G = \mathrm{Gal}(L/K)$ de p sur K vu comme un groupe de permutations sur $\{\xi_i\}$.

En admettant que la décomposition en facteurs premiers dans $\mathbb{Q}[u_1, \ldots, u_d, t]$ est algorithmique, expliquer pourquoi ceci fournit un algorithme théorique permettant de calculer le groupe de Galois de n'importe quel polynôme sur $\mathbb{Q}$ (i.e., le problème du calcul du groupe de Galois est décidable), mais expliquer pourquoi cet algorithme est inutilisable en pratique.

Corrigé. Remarquons tout d'abord que les facteurs $t - \sum_{i=1}^d u_i \xi_{\sigma(i)}$, étant linéaires, sont irréductibles dans $L[u_1, \ldots, u_d, t]$, donc l'expression définissant s donne exactement sa décomposition en facteurs irréductibles dans $L[u_1, \ldots, u_d, t]$. La même chose vaudra pour n'importe quel produit de ces facteurs (et en particulier pour le polynôme g défini ci-dessous).

Le polynôme s est, par construction, totalement invariant par n'importe quelle permutation $\sigma \in \mathfrak{S}_d$ des ξ_i, et notamment par l'action du groupe de Galois $G \leq \mathfrak{S}_d$ de p. Il s'ensuit que s est à coefficients dans le corps fixe par G dans L, c'est-à-dire K ; et plus généralement, cette remarque prouve que le polynôme g défini par $g = \prod_{\sigma \in G} (t - \sum_{i=1}^d u_i \xi_{\sigma(i)})$ est aussi à coefficients dans K (et c'est manifestement un facteur de s).

Comme $\sum_{i=1}^d u_i \xi_{\sigma(i)} = \sum_{i=1}^d u_{\sigma^{-1}(i)} \xi_i$, on peut encore réécrire s comme $s = \prod_{\sigma \in \mathfrak{S}_d} (t - \sum_{i=1}^d u_{\sigma(i)} \xi_i)$, donc s est bien invariant par l'action de $\mathfrak{S}_d$ qui permute les variables $u_1, \ldots, u_d$. Pour ce qui est de g, il est pour la même raison fixé au moins par l'action de G. Pour montrer qu'il n'est pas fixé par plus (c'est-à-dire que $S_g = G$ exactement), on observe que si un $\tau \in S_g$ laisse g invariant (en agissant par permutation sur les u_i), il doit permuter les facteurs irréductibles de g, et notamment il envoie $t - \sum_{i=1}^d u_i \xi_i$ sur $t - \sum_{i=1}^d u_i \xi_{\tau^{-1}(i)}$ ce qui prouve que $\tau \in G$.

Dans $L[u_1, \ldots, u_d, t]$, on a signalé que les facteurs irréductibles de s sont manifestement donnés exactement par les $t - \sum_{i=1}^d u_i \xi_{\sigma(i)}$. En particulier, celle de h doit être donnée par un sous-ensemble de ces facteurs ; quitte à permuter les variables u_i (ce qui conjugue le sous-groupe laissant h invariant), on peut supposer que h comporte le facteur $t - \sum_{i=1}^d u_i \xi_i$ (correspondant à $\sigma = \mathrm{id}$). On cherche alors à prouver que $S_h = G$. Étant donné que h est à coefficients dans K, il est invariant par l'action de G agissant sur les ξ_i : puisque h comporte le facteur $t - \sum_{i=1}^d u_i \xi_i$, il est aussi divisible par tous les facteurs $t - \sum_{i=1}^d u_i \xi_{\sigma(i)}$ avec $\sigma \in G$, c'est-à-dire que g divise h (dans $L[u_1, \ldots, u_d, t]$ mais donc aussi dans $K[u_1, \ldots, u_d, t]$, où ces deux polynômes vivent). Or h était supposé irréductible (dans $K[u_1, \ldots, u_d, t]$), et tous deux sont unitaires, donc $g = h$ et $S_h = S_g = G$.

([1]) On rappelle que les anneaux de polynômes sur un corps sont factoriels.

Pour montrer que ceci fournit un algorithme (théorique) de calcul du groupe de Galois, on constate que les coefficients de s s'obtiennent à partir de ceux de p : on peut par exemple calculer le polynôme « universel »

$$\Upsilon = \prod_{\sigma\in\mathfrak{S}_d} \Big(t - \sum_{i=1}^{d} u_i x_{\sigma(i)}\Big) \in \mathbb{Z}[u_1,\dots,u_d,x_1,\dots,x_d,t]$$

qui est totalement symétrique en les $x_1,\dots,x_d$ et s'écrit donc comme polynôme (à coefficients dans $\mathbb{Z}[u_1,\dots,u_d,t]$) des fonctions symétriques élémentaires $\Sigma_1 = x_1+\cdots+x_d,\ \dots,\ \Sigma_d = x_1\cdots x_d$ de ces variables : et en substituant $(-1)^i a_i$ (les coefficients de p) à Σ_i dans Υ on obtient précisément le polynôme s. La factorisation de s est alors algorithmique, et donné n'importe quel facteur irréductible h, il n'y a plus qu'à vérifier quelles permutations des u_i le laissent invariants pour trouver le groupe de Galois de p (à conjugaison près, mais on ne fera pas mieux : le groupe de Galois n'est défini qu'à conjugaison près, correspondant à un choix arbitraire de l'ordre des racines).

Cette méthode est cependant inutilisable en pratique, puisque le polynôme s est de degré $d!$ en $d+1$ variables, ce qui est impossible à gérer au-delà des toutes petites valeurs de d. ✓

Les exercices suivants demandent quelques connaissances en géométrie et/ou en analyse complexe.

2 (extension icosaédrale). On rappelle que le groupe des isométries directes d'un icosaèdre régulier (ou, dualement, d'un dodécaèdre régulier) est le groupe alterné $\mathfrak{A}_5$ sur cinq éléments. En déduire qu'il existe une extension $\mathbb{C}(u)\subseteq\mathbb{C}(z)$, où u est une certaine fonction rationnelle en l'indéterminée z (et transcendante sur $\mathbb{C}$, c'est-à-dire que le corps $\mathbb{C}(u)$ qu'elle engendre est bien isomorphe au corps des fractions rationnelles complexes sur u vue comme une indéterminée) qui soit galoisienne de groupe de Galois $\mathfrak{A}_5$. Pour cela, on pourra voir les sommets de l'icosaèdre comme des points de la sphère de Riemann, et appliquer le lemme d'Artin et le théorème de Lüroth.

Corrigé. Soit $G\leq SO_3(\mathbb{R})$ le groupe des isométries directes laissant invariant un icosaèdre régulier centré à l'origine (et inscrit dans la sphère unité, pour fixer les idées). On sait[2] que $G\cong\mathfrak{A}_5$.

Pour fixer les idées, on identifie la sphère unité dans $\mathbb{R}^3$ avec la sphère de Riemann par projection stéréographique standard (le complexe $z=a+ib$ est identifié avec le point $(\frac{2a}{|z|^2+1}, \frac{2b}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1})$ et ∞ avec le pôle nord) — l'important étant que l'identification soit conforme, i.e., préserve les angles. Notamment, les douze sommets de l'icosaèdre sont identifiés à douze points de la sphère de Riemann.

Dans ce cas, toute rotation de la sphère (i.e., tout élément de $SO_3(\mathbb{R})$) définit une application conforme sur la sphère de Riemann (c'est-à-dire une homographie[3]). Si on note γ l'application en question, la composition $f\mapsto f\circ\gamma$ définit un automorphisme de $\mathbb{C}(z)$ (au-dessus de $\mathbb{C}$) : le groupe $SO_3(\mathbb{R})$, et en particulier le groupe G, agit donc par automorphismes

([2]) La façon standard de voir ce fait est de partitionner les 30 arêtes de l'icosaèdre en cinq blocs de six arêtes, deux arêtes étant dans le même bloc lorsqu'elles sont parallèles ou orthogonales (sur un dessin c'est plus clair...) : alors une isométrie doit agir en permutant les blocs et on vérifie facilement sur un système quelconque de générateurs qu'on obtient bien le groupe alterné sur les blocs.

([3]) En fait, $SO_3(\mathbb{R})\cong PSU_2$, non seulement comme groupes abstraits mais aussi pour l'action sur la sphère de Riemann, où PSU_2 est le groupe des matrices 2×2 unitaires de déterminant 1, modulo $\{\pm I\}$, agissant sur la sphère de Riemann par $\begin{pmatrix} a & b\\ c & d\end{pmatrix}\cdot z\mapsto\frac{az+b}{cz+d}$ (sous-groupe du groupe $PGL_2(\mathbb{C})$ de toutes les homographies, donc).

sur $\mathbb{C}(z)$, et cette action est évidemment fidèle (si l'action d'un élément est triviale, elle est en particulier triviale sur l'indéterminée z elle-même, c'est-à-dire que $\gamma = \mathrm{id}$).

On a donc plongé G comme un groupe d'automorphismes sur $\mathbb{C}(z)$. Si F est le corps fixe, le lemme d'Artin assure que $F \subsetneq \mathbb{C}(z)$ est une extension galoisienne de groupe G, et le théorème de Lüroth garantit que F s'écrit $\mathbb{C}(u)$ pour $u \in \mathbb{C}(z)$ transcendant sur $\mathbb{C}$. C'est tout ce qui était demandé.

On peut en fait en dire un peu plus : la fonction rationnelle u est, par définition, invariante sous l'action de G, donc constante sur chaque orbite de G sur la sphère de Riemann. Comme l'orbite générale de G a pour cardinal 60, et que u n'est certainement pas constante, le degré[4] de u est au moins 60 ; et ce n'est pas moins de 60 car $\prod \gamma(z)$ (produit sur tous les éléments de G) définit un invariant de degré 60. L'indice de ramification de u est alors 5 en chacun des 12 sommets de l'icosaèdre, 2 en chacun des milieux des 30 arêtes, et 3 en chacun des centres des 20 faces, et quitte à composer à gauche par une homographie on peut supposer que u vaut respectivement 0, 1 et ∞ en ces points, ce qui le détermine complètement. Un calcul explicite est alors possible : $u = -\dfrac{1728\, z^5\, (z^{10} + 11z^5 - 1)^5}{(z^{20} - 228z^{15} + 494z^{10} + 228z^5 + 1)^3}$ pour un placement standard de l'icosaèdre (ce n'est pas aussi difficile qu'il y paraît : cf. le livre de Jerry Shurman, *The Geometry of the Quintic* chapitres 2–3). ✓

3 (problème de Galois inverse pour $\mathbb{C}(z)$). On se propose de démontrer que tout groupe fini est le groupe de Galois d'une extension (galoisienne finie) de $\mathbb{C}(z)$.

Soit G un groupe fini, d'ordre n, et $g_1 = 1, \ldots, g_n$ ses éléments. On considère l'ensemble E des données $t = (t_1, \ldots, t_n)$ suivantes : pour chaque $i \in \{1, \ldots, n\}$, une fonction t_i *méromorphe* sur $\mathbb{C} \setminus [1; n]$ (où $[1; n]$ désigne l'intervalle fermé réel ayant ces bornes), à croissance au plus polynomiale à l'infini (c'est-à-dire $|t_i(z)| = O(|z|^k)$ pour un certain k lorsque $|z| \to +\infty$) ainsi qu'en tout point du bord (c'est-à-dire $|t_i(z - c)| = O(|z - c|^{-k})$ lorsque $z \to c$ avec $c \in [1; n]$), et vérifiant de plus la condition de compatibilité suivante : pour chaque triplet (i, j, k) tel que $g_i g_j = g_k$ dans G, la fonction t_i restreinte au demi-plan supérieur $\{z : \Im z > 0\}$ et la fonction t_k restreinte au demi-plan inférieur $\{z : \Im z < 0\}$ se prolongent en une fonction méromorphe commune sur un voisinage de $]j - 1; j[$ dans le plan complexe (lorsque $j = 1$, bien sûr, cette condition est automatique).

(a) Expliquer pourquoi E est un corps (l'addition et la multiplication étant données par les opérations terme à terme sur les t_i). On montrera notamment que si un quelconque des t_i associés à un $t \in E$ est nulle (ou simplement nulle sur un ouvert non vide) alors tous les t_i sont nuls.

(b) On plonge $\mathbb{C}(z)$ dans E en identifiant une fonction rationnelle $h \in \mathbb{C}(z)$ avec le n-uplet $(h, \ldots, h)$ où chaque composante est la fonction h elle-même (vue comme une fonction méromorphe sur $\mathbb{C}$, donc *a fortiori* sur $\mathbb{C} \setminus [1; n]$). Expliquer pourquoi ce plongement est correct (définit bien un élément de E).

(c) On fait agir G sur E en posant $g \cdot (t_1, \ldots, t_n) = (t'_1, \ldots, t'_n)$, où $t'_i = t_{i'}$ si $g_{i'} = g g_i$: expliquer pourquoi cette action a un sens. Expliquer pourquoi le corps fixe de E par G est exactement $\mathbb{C}(z)$.

(d) On *admet*[5] le fait suivant : pour tout $i \in \{2, \ldots, n\}$, il existe $t \in E$ tel que $t_i(0) \neq t_1(0)$. Montrer alors que E est bien une extension de $\mathbb{C}(z)$ galoisienne de groupe de Galois G.

([4]) Le degré d'un élément de $\mathbb{C}(z)$ est le maximum du degré de son numérateur et de son dénominateur réduits, c'est-à-dire le nombre d'antécédents d'un complexe suffisamment général par cette fraction.

([5]) Il s'agit d'une conséquence du théorème de séparation de Riemann (sur toute surface de Riemann — compacte —, les fonctions méromorphes séparent les points). Reconnaissons que, dans ce cas, c'est un peu une pétition de principe, puisque toute la difficulté du résultat est cachée dans ce fait admis.

Corrigé. (a) Le fait que E soit un anneau ne pose pas de difficulté (c'est un sous-anneau du produit de n copies de l'anneau des fonctions méromorphes sur $\mathbb{C} \setminus [1;n]$).

Par ailleurs, si un certain $t \in E$ vérifie $t_i = 0$ (il suffit bien sûr que t_i s'annule sur un certain ouvert non vide dans $\mathbb{C} \setminus [1;n]$, ce dernier étant connexe) alors $t_k = 0$ pour tout k puisque dès que $g_i g_j = g_k$ les fonctions t_i et t_k sont réputées être prolongeables en une fonction méromorphe commune — qui doit donc être nulle — sur un certain ouvert contenant $]j-1;j[$. On a donc prouvé que pour tout $t \in E$ non nul aucune des fonctions t_i n'est nulle, donc t est inversible. Bref, E est bien un corps.

(b) Une fonction rationnelle $h \in \mathbb{C}(z)$ a croissance polynomiale en tout point complexe, ainsi qu'à l'infini. Par ailleurs, les conditions de recollement sont évidentes, donc $(h,\dots,h)$ définit bien un élément de E. Et comme les opérations sur E sont définies terme à terme, on a bien plongé ainsi $\mathbb{C}(z)$ dans E.

(c) Il s'agit de vérifier que les conditions de compatibilité sont encore vérifiées par $(t'_1,\dots,t'_n)$ si $g \cdot t = t'$ avec $t \in E$. Or si $g_i g_j = g_k$ dans G, on a $g g_i g_j = g g_k$, c'est-à-dire $g_{i'} g_j = g_{k'}$ où $g_{i'} = g g_i$ et $g_{k'} = g g_k$: ainsi, $t'_i = t_{i'}$ et $t'_k = t_{k'}$ se prolongent bien, au voisinage de $]j-1;j[$, en une fonction méromorphe commune.

Par ailleurs, il s'agit bien d'une action car si $t \in E$ et $g,h \in G$, on a $(hg)\cdot t = t''$ où $t''_\ell = t_{hg\ell}$ (ici on a identifié de façon évidente l'élément g_i de G avec son indice i) et c'est bien $h \cdot (g \cdot t)$.

Enfin, si $t \in E$ est fixe par G, tous les t_i sont égaux, donc définissent une unique fonction méromorphe sur $\mathbb{C} \setminus \{1,\dots,n\}$. Mais les conditions de croissance polynomiale aux points $c \in \{1,\dots,n\}$ prouvent que cette fonction est prolongeable en une fonction méromorphe encore en ces points (en effet, quitte à multiplier par une puissance suffisante de $z-c$ la fonction devient bornée au voisinage de c, donc holomorphe sur un voisinage de ce point), i.e., elle n'a pas de singularité essentielle. Et comme elle n'a pas non plus de singularité essentielle à l'infini complexe (de même car elle y a une croissance polynomiale), le théorème de Liouville montre qu'elle est rationnelle : soit $t \in \mathbb{C}(z)$.

(d) Le fait admis garantit que G agit ***fidèlement*** sur E (si $t_1(0) \neq t_i(0)$ alors g_i ne laisse pas t fixe). C'est-à-dire que G peut être considéré comme un sous-groupe du groupe de automorphismes du corps E. Comme le corps fixe est $\mathbb{C}(z)$, le lemme d'Artin assure que $\mathbb{C}(z) \subseteq E$ est une extension galoisienne de groupe G. ✓

Remarque : Le principe utilisé dans ce dernier exercice est de construire — sans le dire — un revêtement ramifié de la sphère de Riemann ayant $\{1,\dots,n\}$ pour points de ramification et groupe de Galois G, et le corps E est simplement le corps des fonctions méromorphes sur ce revêtement.